(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001117873 A**

(43) Date of publication of application: **27.04.01**

(51) Int. Cl **G06F 15/00**
G06F 19/00
G07F 19/00

(21) Application number: **11296257**

(22) Date of filing: **19.10.99**

(71) Applicant: **HITACHI LTD**

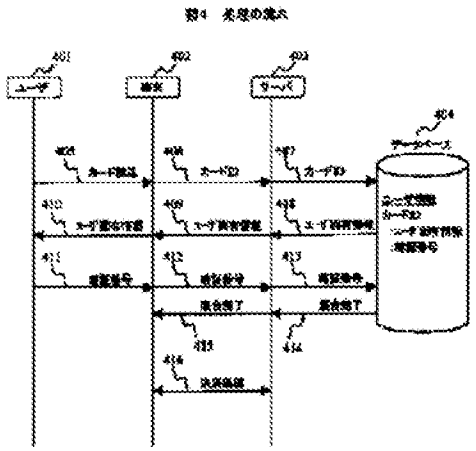
(72) Inventor: **TAKAHASHI YASUHIRO**
MATSUI SUSUMU

(54) **METHOD FOR IDENTIFYING TERMINAL**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent information such as a personal code number or a password from being stolen by inputting the information without knowing that the terminal or a system is the false one in card settlement or a server access.

SOLUTION: Card information and a user ID are inputted in the terminal and transmitted to a server. The server transmits information intrinsic to a user, which is only known to the user, to the terminal from the information and it is displayed. The user confirms the information transmitted from the server, i.e., the second password and, then, inputs the password which he does not want others to know.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－117873
（P2001－117873A）
(43)公開日　平成13年４月27日(2001.4.27)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	15/00	３３０	Ｃ０６Ｆ 15/00	３３０Ｂ	３Ｅ０４０
	19/00		15/30	３３０	５Ｂ０５５
Ｇ０７Ｆ	19/00			３４０	５Ｂ０８５
			Ｇ０７Ｄ 9/00	４７６	９Ａ００１

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－296257

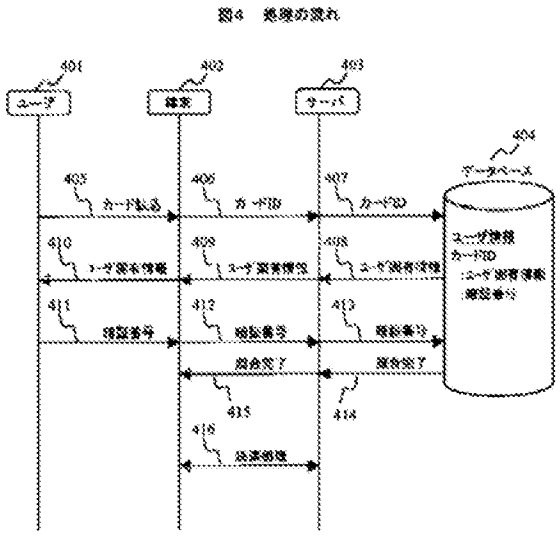
(22)出願日　平成11年10月19日(1999.10.19)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　高橋　泰弘
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　松井　進
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　端末識別方法

(57)【要約】
【課題】カード決済や、サーバアクセスにおいて、偽物の端末やシステムとは知らずに、暗証番号やパスワードを入力してしまい、これらの情報を盗まれてしまうことを防止する。
【解決手段】端末において、カード情報や、ユーザＩＤを入力し、これをサーバに送り、サーバはこれらの情報から、ユーザしか知らないユーザ固有の情報を端末に送り表示させる。ユーザは、サーバから送られるこの情報、言わば第２の暗証番号を確認した上で、ユーザは他人に知られたくない暗証番号を入力する。



【特許請求の範囲】
【請求項１】端末利用者から入力される第1の情報によって、端末利用者の認証を行なうための端末であって、前記第1の情報を端末利用者が入力する前に入力される前記端末利用者によって入力される第２の情報に応じて、前記端末利用者が予め把握している第3の情報を出力する出力手段と、前記出力手段が第3の情報を出力したのち前記端末利用者から前記第1の情報の入力を可能とする入力手段とを有し、前記出力手段は前記入力手段から入力される第1の情報に基づく前記端末利用者の認証結果を出力することを特徴とする端末。
【請求項２】請求項１に記載の端末において、
前記第1の情報は、暗証番号或いはパスワードであり、前記第2の情報は、前記端末利用者を特定する情報であるユーザ識別ＩＤであり、前記第3の情報は前記端末利用者が前記第2の情報と前記第3の情報との対応関係を予め把握しうるユーザ固有情報であることを特徴とする端末。
【請求項３】請求項２に記載の端末において、
前記第3の情報は、各端末利用者に対し複数のユーザ固有情報からなり、前記入力手段は前記端末利用者から前記複数のユーザ固有情報から一つのユーザ固有情報を指示する指示情報を入力し、前記出力手段は前記入力手段からの指示情報に基づいて選択されるユーザ固有情報を出力することを特徴とする端末。
【請求項４】請求項２に記載の端末において、
前記出力手段は、前記ユーザ固有情報を表示するものであることを特徴とする端末。
【請求項５】端末利用者から入力される第1の情報によって、端末利用者の認証を行なう端末にネットワークを介して接続される情報処理装置であって、前記第1の情報に対応する第3の情報を複数組み記憶する記憶手段と、前記端末利用者が前記第1の情報を入力する前に前記端末から受信した第２の情報に応じて、前記端末利用者が予め把握している第3の情報を検索する手段と、前記検索した第3の情報を前記端末に送信する手段と、前記第3の情報を前記端末に出力したのち前記端末から受信した前記第1の情報により、前記端末利用者の認証を行なう手段とを有することを特徴とする情報処理装置。
【請求項６】請求項５に記載の端末において、
前記第1の情報は、暗証番号或いはパスワードであり、前記第2の情報は、前記端末利用者を特定する情報であるユーザ識別ＩＤであり、前記第3の情報は前記端末利用者が前記第2の情報と前記第3の情報との対応関係を予め把握しうるユーザ固有情報であり、前記記憶手段は、各端末利用者に対し複数のユーザ固有情報を記憶しており、前記検索手段は前記端末から受信した指示情報に応じて前記複数のユーザ固有情報の内の一つを検索することを特徴とする情報処理装置。
【請求項７】端末利用者から入力される第1の情報によって、端末利用者の認証を行なう利用者認証システムであって、前記第1の情報を前記端末利用者に入力させる端末と、前記端末にネットワークを介して接続される情報処理装置とを有し、
前記端末は、前記端末利用者から前記第1の情報の入力に先立って第2の情報を入力し、前記情報処理装置に送信し、
前記情報処理装置は、前記第２の情報に対応する第3の情報を複数組み記憶する記憶手段を有しており、前記端末から受信した前記第2の情報に応じて、前記端末利用者が予め把握している第3の情報を検索し、前記検索した結果を前記端末に送信し、
前記検索された第3の情報を受信した端末は、更に、前記端末利用者から第1の情報を受け取り、前記情報処理装置に送信し、
前記端末から第1の情報を受信した前記情報処理装置は、前記第1の情報に基づいて前記端末利用者の認証を行なうことを特徴とする利用者認証システム。
【請求項８】請求項７記載の利用者認証システムにおいて、
前記第1の情報は、暗証番号或いはパスワードであり、前記第2の情報は、前記端末利用者を特定する情報であるユーザ識別ＩＤであり、前記第3の情報は前記端末利用者が前記第2の情報と前記第3の情報との対応関係を予め把握しうるユーザ固有情報であることを特徴とする利用者認証システム。
【請求項９】利用者が端末に暗証番号或いはパスワードを入力する前に、前記利用者に前記端末が真正なものであることを知らせることを特徴とする利用者認証方法。
【請求項１０】利用者から入力される暗証番号或いはパスワードよって、利用者の認証を行なう利用者認証方法であって、
前記利用者から前記暗証番号或いはパスワードの入力に先立って、前記利用者からのユーザ識別ＩＤを入力し、
前記暗証番号或いはパスワードに対応するユーザ固有情報を複数組み記憶しており、前記ユーザ識別ＩＤに応じて、前記利用者が予め把握しているユーザ固有情報を検索し、
前記検索されたユーザ固有情報を前記利用者が認識できる表示あるいは音声として出力したのち、前記利用者から暗証番号或いはパスワードを受け取り、
前記受け取った暗証番号或いはパスワードに基づいて前記利用者の認証を行なうことを特徴とする利用者認証方法。
【請求項１１】請求項9または１０の何れか記載の利用者認証方法において、
前記ユーザ固有情報は、各利用者に対し、複数記憶されており、
前記各利用者から入力される指示情報に基づいて、前記複数のユーザ固有情報のうちの一つを選択することを特

徴とする利用者認証方法、

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ通信に関し、とくに、端末となる計算機から、データ通信を行い、サーバにアクセスする際の、ユーザを認証する際、ユーザが使用する計算機やサーバの正当性を確認する方法、端末、サーバ、システムに関わる。

【０００２】

【従来の技術】従来、端末とサーバからなるシステムにおいて、サーバが端末やそのユーザを正規のものかを認証することや、あるいは、端末が接続先のサーバが正しいサーバであるかを認証することは行われていた。

【０００３】例えば、端末とサーバが正しいものであるかを互いにチェックする工夫は、特開平１１－８５７０２号公報に記載されているように、端末とサーバ間のやりとりの中で、予め用意しておいた暗証番号のうちの1つをユーザに入力させ、互いの正当性を確認しあっていた。

【０００４】また、従来、暗証番号やパスワードを入力時に第三者から盗み見られないような工夫はあった。

【０００５】例えば、現金自動取引機においては、カード情報と暗証番号の組み合わせで、ユーザ認証する方法が一般的であり、特開平１１－１９１０９４号公報に記載されているように、暗証番号を入力する際に、表示を変えたり、キー操作がわからないようにするなどして、他人から盗み見られないように工夫されていた。

【０００６】

【発明が解決しようとする課題】上記、端末とサーバが正しいものであるかを互いにチェック方法においては、暗証番号を入力するユーザには、正しいサーバに接続されているのかや、端末が正規のものであるかは、正しくは確認できないため、機械そのものが偽物であることで、暗証番号を盗まれる危険性に対する対処にはなっていなかった。

【０００７】また、暗証番号やパスワードを入力時に第三者から盗み見られないような工夫においては、現金自動取引機は正しい機械であるということが前提となっていたため、ユーザは機械を信用して、その指示に従うままに、暗証番号を入力していた。そのため、機械そのものが偽物であることで、暗証番号を盗まれる危険性に対する対処はなかった。

【０００８】特に、今後、タクシーや、臨時店舗など、さまざまな場所で、多種多様な端末を使用して、決済処理を行うケースが増えてくるが、ユーザは、その端末、あるいは、接続されているサーバやシステムが正しいものであるのか、あるいは、カード情報や暗証番号を盗む目的で作られた偽端末あるいは偽システムであるかは、現状のカードを差込み、そのまま暗証番号を入力する方法では、見破ることは不可能であった。

【０００９】本発明の目的は、電子商取引やデビットカードによる電子決済において、端末、もしくは、端末に接続しているサーバが偽物であるために、暗証番号を他人に盗まれてしまうことを未然に防止する識別方法、端末、サーバ、システムを提供することにある。

【００１０】

【課題を解決するための手段】上記目的を達成するために、本発明では、カードの挿入や、ユーザＩＤや口座番号などの入力により、その情報をサーバに伝える手段と、サーバはこの入力情報から、ユーザにしかわからないユーザ固有の情報を端末に送信し表示する手段と、ユーザは送信されてきたユーザ固有の情報を読む、見る、あるいは、聞き、正しい内容であることを認識することで、端末とサーバが正当であることを確認してから、暗証番号を入力し、サーバに送信する手段を設ける。

【００１１】すなわち、他人には漏らしたくない暗証番号を入力する前に、該端末やシステムが正規のものであるかを、ユーザが判断する情報をシステムが提供する仕組みを用意することで解決する。その判断のための情報として、あらかじめユーザが正規のサーバに登録しておいたユーザ固有の情報を、端末に表示し、ユーザに示すことにより、正規のものか、偽物かを、ユーザが判断できるようにする。

【００１２】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

【００１３】図1は、本発明の一実施例を示すシステム構成図である。

【００１４】この図においては、101はユーザ、102は端末、103はネットワーク、104はサーバ、105はユーザ情報を格納するデータベース、106は決済センタを示す。

【００１５】ユーザ101が、端末102を使用して、遠隔地から、決済処理を行う場合、ネットワーク103を利用し、決済センタ106内のサーバ104にアクセスし、ユーザの情報が蓄積されているデータベース105を用いて、認証処理を行った後に、決済の処理を行うものである。この例では、主として、ユーザは決済処理を行うにあたって、カードを使用し、暗証番号又はパスワード（以下、単に暗証番号と記す）を入力することで、その情報が、決済センタのサーバに届き、サーバ内の登録データと照合することで、本人であることの証明を行い、決済処理を行う。

【００１６】図2は、端末およびサーバ構成図を示している。

【００１７】この図に示すように、端末101は、表示部201、CPU 202、メモリ203、カードリーダ204、キー入力部205、通信ポート206とを有する。決済センタ106は、サーバ104と、データベース105とを有する。サーバ104は、入力装置208、表示部209、CPU 210、メモリ211、通信ポート212とを有する。データベース105は、蓄積装置

214から構成されている。サーバ104とデータベース105は、バス213にて接続されている。端末101とサーバ104は、ネットワーク103で接続されている。

【0018】端末101は、メモリ203に蓄えられているプログラムをCPU 202が実行し、カードリーダ204の制御や、表示部201での表示、キー入力205からの入力、通信ポート206を通じてのサーバとの通信を行う。

【0019】サーバ104は、メモリ211に蓄えられているプログラムをCPU 210が実行し、通信ポート206を通じての端末との通信、データベース105へのアクセス、表示部209での表示、入力装置208からの入力、を行う。

【0020】データベース105は、サーバ104でのプログラム実行のもとで、データの検索、照合を行う。

【0021】図3は、本発明を適用した端末での画面表示を示した図である。

【0022】端末画面301aから301dは、処理の流れにそった画面表示を示している。最初に、端末画面301aにおいて、「カードを読込ませてください」という表示302が出る。これにより、303に示しているように、ユーザは、端末のカードリーダでカード情報を読込ませる。次に、カード情報がサーバに送信され、このカード情報からデータベースより検索されたユーザ固有情報がサーバから端末へ送られてくる。端末画面301bに示すように、ユーザ固有情報304が表示され、ユーザがこれを正しい値だと判断し、ＯＫボタン305を押すと、画面は、端末画面301cに変わる。端末画面301cでは、「暗証番号を入れてください」という表示306が出る。

【0023】これにより、ユーザは、端末画面301dに示すように、暗証番号307を入力する。

【0024】続いて、308に示すように、入力された暗証番号がサーバに送られ、決済処理が行われる。端末画面301aにおいて、カードの挿入が指示された後に、端末画面301bにおいて、ユーザ固有情報が表示されることにある。ユーザは、この表示されたユーザ固有情報を見て、事前に決済センタに自分が登録しておいたものかどうかを判断し、正しい値であった場合のみ、端末301dで暗証番号を入力というものである。

【0025】ここで、もし、ユーザ固有情報が表示されずに、そのまま、暗証番号の入力を指示する画面が出たり、あるいは、ユーザ固有情報は表示されたが、表示された値が間違ったものであった場合には、使用している端末、もしくは、接続しているサーバが不正なものであると、ユーザが判断でき、暗証番号を入力しないで済むので、暗証番号を盗まれることを未然に防ぐことができるものである。

【0026】図4は、ユーザ、端末、サーバ、データベースの間での処理の流れを示した図である。

【0027】ユーザ401が、405に示すように、カードを端末402に読込ませると、端末は、406が示すように、読込んだカード情報内のカードIDをサーバ403に伝える。ここで、カードＩＤはユーザを特定し得る情報である名称、記号、番号等であればよい。この意味でカードＩＤは図5に示す口座番号、ユーザＩＤ等の概念を含むユーザ識別ＩＤとして機能する。

【0028】サーバ403は、407に示すように、カードIDをデータベース404に伝える。データベース404では、蓄積されているユーザ情報から、カードIDをキーに、ユーザ固有情報を検索し、408に示すように、サーバ403に伝える。ここで、ユーザ固有情報とは、先のユーザ識別ＩＤによって一義的に特定され、ユーザによって予め認識されている名称、番号、記号、音声等の情報である。

【0029】サーバ403は、409に示すように、ユーザ固有情報を端末402に伝える。端末402は、410に示すように、ユーザ固有情報を表示し、ユーザ401に知らせる。ユーザ401は、表示されたユーザ固有情報が正しいものであるかどうかを見て、判断し、正しい場合には、411に示すように、暗証番号を端末402に入力する。端末402は、412に示すように、暗証番号をサーバ403に伝える。サーバ403は、413に示すように、暗証番号をデータベース404に伝える。データベース404では、伝えられた暗証番号が、データベース内のユーザ情報に、あらかじめ登録してある暗証番号と一致するかどうかの照合を行う。一致する場合は、414に示すように、サーバ403に対して、照合完了の通知と結果を伝える。サーバ403では、415に示すように、端末402に対して、照合完了を通知すると共に、一致していた場合には、端末402とサーバ403において、決済処理416を開始する。

【0030】図5は、決済センタ内のデータベースに蓄積されているユーザ情報管理テーブルであり、ユーザ識別ID 501と、ユーザ固有情報502と、暗証番号503からなる。

【0031】ユーザ識別ID 501は、例えば、カードIDや、口座番号や、ユーザIDなどが用いられる。このユーザ情報管理テーブル500は、ユーザ識別ID 501をキーに、ユーザ固有情報502や、暗証番号503を検索できるようになっている。

【0032】図6は、本発明における「ユーザ」から見た処理フローを示した図である。

【0033】処理601において、端末から、カードの入力の要求があると、処理602において、ユーザは、カードを読込ませる602。次に、処理603において、端末が表示するユーザ固有情報が正しいものかどうかを見て判断し、正しければ、処理604において、ＯＫボタンを押す。次に、処理605のように、端末が暗証番号の入力を求めてきたら、処理606において、暗証番号を入力し、その後、処理607において、決済サービスを受ける。

【0034】一方、処理603において、ユーザ固有情報が表示されなかったり、表示された情報が正しいものでなかった場合には、処理608において、操作を止め、処理609のように、使用した端末が偽端末であるか、また

は、偽システムに接続されていると判断し、暗証番号を入力することなく、処理を終える。

【００３５】図7は、本発明における「端末」によって実行される処理フローを示した図である。ここに示す機能は、プログラムとして実現される。

【００３６】処理701において、カードの挿入待ちをしており、カード挿入があると、処理702において、ユーザ識別ＩＤを含むカード情報を読込む。読込んだカード情報を、処理703において、決済センタのサーバへ送信する。次に、処理704において、サーバからユーザ固有情報の受信を待ち、受信があると、処理705において、ユーザ固有情報を端末の画面に表示する。次に、処理706に示すように、ユーザがＯＫのボタンを押したら、処理707において、ユーザに対して、暗証番号の入力要求を端末画面に表示させる。処理708において、ユーザによる暗証番号の入力があった場合には、処理709において、決済センタのサーバへ、入力された暗証番号を送信する。次に、処理710において、サーバでの認証完了を待ち、完了した場合には、処理711で認証の結果を調べ、ＯＫなら、処理712において、決済サービスを開始させ、処理713において、サービスが終了したら、はじめの状態に戻る。

【００３７】一方、処理711において、認証結果がＮＧの場合には、処理714のように、取引中止の措置をとり、はじめの状態に戻る。

【００３８】図8は、本発明における「サーバ」によって実行される処理フローを示した図である。ここに示す機能は、プログラムとして実現される。

【００３９】処理801において、端末からのユーザ識別ＩＤを含むカード情報の受信待ちを行い、受信した場合には、処理802において、受信したカード情報をデータベースに送り、ユーザ固有情報の検索を指示する。次に、処理803において、データベースからのユーザ固有情報の検索待ちを行い、検索完了時には、処理804において、検索されたユーザ固有情報の、端末への送信を行う。次に、処理805において、端末からの暗証番号を待ち、受信があったら、処理806において、受信した暗証番号をデータベースに送り、データベース内にあらかじめ登録してある暗証番号と一致するかどうかの照合処理を指示する。処理807において、データベースでの照合処理が完了したことがわかった場合、処理808において、照合結果を調べ、ＯＫなら、処理810において、決済サービスを開始させ、処理811において、サービスが終了したら、はじめの状態に戻る。

【００４０】一方、処理808において、照合結果がＮＧの場合には、処理812のように、取引中止の指示を出す措置をとり、はじめの状態に戻る。

【００４１】図9は、本発明における「データベース」の処理フローを示した図である。ここに示す機能は、プログラムとして実現される。

【００４２】処理901において、サーバからの検索依頼を待ち、依頼があった場合には、処理902において、依頼の内容が、ユーザ識別ＩＤを含むカード情報をキーとしたユーザ固有情報の検索依頼なのかを調べ、そうである場合は、処理903において、ユーザ情報管理テーブルに対して、カード情報をキーにユーザ固有情報を検索する。そして、処理904において、検索結果のユーザ固有情報をサーバへ送信し、はじめに戻る。

【００４３】一方、処理902において、依頼内容が、ユーザ固有情報の検索でない場合には、処理905において、依頼内容が、ユーザ識別情報を含むカード情報をキーとした暗証番号の照合依頼であったのかどうかを調べる。そうである場合には、処理906で、ユーザ情報管理テーブルに対して、カード情報をキーに暗証番号を検索する。そして、処理907において、サーバからの暗証番号と、検索した暗証番号が一致するかどうかを調べ、一致する場合には、処理908において、照合完了処理を行い、照合結果が「一致」である旨をサーバへ通知し、はじめに戻る。

【００４４】一方、処理907において、サーバからの暗証番号と、検索した暗証番号が一致しない場合には、処理909において、照合完了処理を行い、照合結果が「不一致」である旨をサーバへ通知し、はじめに戻る。

【００４５】また、処理905において、依頼内容がいずれにも該当しない場合には、はじめに戻る。

【００４６】図１０は、使用している端末が偽端末であった場合に、不正と判断し、取引を中止させるにいたるまでの処理の流れを示した図である。

【００４７】ユーザ1001が、端末（偽端末）1002に、1003のように、カードを読込ませるが、端末が偽物であるため、正規のサーバへ接続することもできず、返すべき、ユーザ固有情報もわからないために、1004のように、ユーザ固有情報以外の表示を行った場合、ユーザは、処理1005において、不正と判断し、取引を中止する。

【００４８】同様に、ユーザ1006が、端末（偽端末）1007に、1008のように、カードを読込ませるが、端末が偽物であるため、正規のサーバへ接続することもできず、返すべき、ユーザ固有情報もわからないために、1009のように、正しくないユーザ固有情報の表示を行った場合、ユーザは、処理1010において、不正と判断し、取引を中止する。

【００４９】図１１は、接続したサーバが偽サーバであった場合に、不正と判断し、取引を中止させるにいたるまでの処理の流れを示した図である。尚、偽サーバは、当然のこととして正規なデータベースにアクセスできるものではない。そのため、偽サーバは図5に示したようなユーザ識別ＩＤとユーザ固有情報との関係を把握することができず、端末１１０２から受け取ったカードＩＤから正規なユーザ固有情報を検索することはできない。

【００５０】ユーザ1101が、端末1102に、1105のように、カードを読込ませる。端末1102は、接続したサーバ（偽サーバ）1103に、1106のように、カードＩＤ等のユーザ識別ＩＤを伝え、偽サーバ1103がこれを受け取り、データベース1104にて、ユーザ固有情報を検索しようとするが、正しい値が登録されていないので、偽サーバ1103には，1108のように、正しくないユーザ固有情報が伝わる。偽サーバ1103は、さらにこの正しくないユーザ固有情報を、処理1109のように、端末1102に伝え、さらに、端末1102は、処理1110のように、その正しくないユーザ固有情報を端末の表示部において表示させ、ユーザに処理を促す。ユーザ1101は、処理1111のように、不正と判断し、取引中止の措置をとる。

【００５１】次に示す実施例は、ユーザ固有情報を音声でユーザに知らせる場合の実施例である。

【００５２】図１２は、音声にて、端末あるいは、接続しているサーバが本物か偽物かどうかを識別する場合の端末およびサーバの構成図であり、端末101、決済センタ106、サーバ104、データベース105から構成される。

【００５３】端末101には、音声出力部1201が備えられ、これには、ヘッドフォン1202が接続できるようになっている。端末のCPU 202において、サーバ104より受信したユーザ固有情報を、音声に変換し、音声出力1201で再生し、ユーザが正しいユーザ固有情報か否かを判断する。ヘッドフォン1202は、第３者に、読み上げられた情報を聞かれないようにするためのものである。

【００５４】端末における画面表示だけなく、音声でも視聴できるようにすることによって、視覚障害者にも使いやすいシステムとなる。

【００５５】次に示す実施例は、ユーザ固有情報を複数登録できるようにし、必要に応じて、確認手段を変えることができ、安全性を高めた場合の実施例である。

【００５６】図１３は、ユーザ固有情報が複数の場合の，データベースに蓄積されるユーザ情報管理テーブルを示した図であり、ユーザ識別ID 1301と，ユーザ指示情報1302と、ユーザ固有情報1303と、暗証番号1304からなる。

【００５７】ユーザ識別ID 1301は、例えば，カードIDや，口座番号や、ユーザIDなどが用いられる。１つのユーザ識別IDに対しては，複数のユーザ固有情報を登録でき，どのユーザ固有情報を読み出すかは、ユーザが、ユーザ指示情報1302を指定することで、それに対応するユーザ固有情報1303が読み出される。すなわち，ユーザ固有情報1303については、ユーザ識別ID 1301と、ユーザ指示情報1302がキーとなって検索が行われるようになっており，該当するユーザ固有情報1303が読み出される。

【００５８】ユーザ固有情報を複数用意し、ユーザ提示情報1302で指定できるので、ユーザは必要に応じて，確認に用いる値を変更することができるようになるため、万一、ユーザ固有情報が他人に知られても，他のユーザ固有情報を用いて，端末を正規のものか否かを確認する手段があるため、安全性が向上する。普段使用しているユーザ固有情報が盗まれたと判断した場合には、ユーザ指示情報で，別のユーザ固有情報を選択できるようにすることで，暗証番号までも，盗まれることを防ぐことが可能となる。

【００５９】図１４は、ユーザ固有情報が複数の場合の，端末画面を示した図である。

【００６０】端末画面1401aから端末画面1401fにおいて、カードを読込ませた後，ユーザに、ユーザの意図するユーザ固有情報を表示させるために、指示情報の入力を促し、その後、その指示情報にあったユーザ固有情報を表示させるものである。

【００６１】端末画面1401bでは、カード入力の後に、指示情報の入力を促す画面1403が表示され，ユーザは、端末画面1401cにおいて、指示情報1404を入力する。これにより、端末画面1401dにおいて、対応するユーザ固有情報1405が表示され、正規のものか否かをユーザは判断できる。

【００６２】図１５は、ユーザ固有情報が，複数ある場合の処理の流れを示した図である。

【００６３】ユーザ、端末、サーバ、データベースの間での処理の流れを示している。

【００６４】ユーザ1501が、1505に示すように、カードを端末1502に読込ませると、端末は、1506が示すように，読込んだカード情報内のカードIDをサーバ1503に伝える。サーバ1503は，1507に示すように，カードIDをデータベース1504に伝える。

【００６５】さらに、ユーザ1501は，1508に示すように，ユーザ指示情報を端末1502に入力すると，端末は，1509が示すように，入力されたユーザ指示情報をサーバ1503に伝える。サーバ1503は，1510に示すように，入力されたユーザ指示情報をデータベース1504に伝える。

【００６６】データベース1504では，蓄積されているユーザ情報から，カードIDとユーザ指示情報をキーに，ユーザ固有情報を検索し，1511に示すように，サーバ1503に伝える。サーバ1503は，1512に示すように，ユーザ固有情報を端末1502に伝える。端末1502は，1513に示すように，ユーザ固有情報を表示し，ユーザ1501に知らせる。ユーザ1501は，表示されたユーザ固有情報が正しいものであるかどうかを見て，判断し，正しい場合には，1514に示すように，暗証番号を端末1502に入力する。

【００６７】図１６は、認証局を含めた認証処理に、本発明が適用した認証局を含めたシステム構成図である。

【００６８】101はユーザ，102は端末，103はネットワーク，104はサーバ，105はユーザ情報を格納するデータベース，106は決済センタ，そして，1601は認証局を示す。

【００６９】端末102が，サーバ104にカード情報を伝える際に，認証局1601によって，認証を行った上で，本発

明のユーザ固有情報の表示を行い、ユーザが正しい端末であり、正しいサーバに接続していることを確認できるようにした例である。

【００７０】図１７は、図１６のシステムにおける認証局経由の場合の、処理の流れを示した図である。

【００７１】ユーザ、端末、サーバ、データベース、認証局との間での処理の流れを示している。

【００７２】ユーザ1701が、1706に示すように、カードを端末1702に読込ませると、端末は、1707が示すように、読込んだカード情報内のカードIDをサーバ1703に伝える。サーバ1703は、1708に示すように、カードIDを認証局1704に伝える。

【００７３】認証局1704では、蓄積されているユーザ情報から、カードIDをキーに、認証演算情報を検索し、1709に示すように、生成したチャレンジコードをサーバ1703に伝える。サーバ1703は、1710に示すように、チャレンジコードを端末1702に伝える。端末1702は、1711に示すように、チャレンジコードに対するレスポンスコードを演算し、サーバ1703に返す。サーバ1703は、1712に示すように、端末1702からのレスポンスコードを認証局1704に渡す。認証局1704では、サーバ1703より受け取ったレスポンスコードを調べ、1713のように認証結果として、サーバ1703に渡す。サーバ1703は受け取った認証結果が正当なものであるとする内容である場合には、先に端末より受け取ったカードIDを、1714のように、データベース1705に渡す。サーバ１７０３が受け取った認証結果の内容が正当なものであるとする内容でない場合、端末１７０２から受け取ったカードＩＤをデータベースに送ることなく、処理を終了する。

【００７４】サーバ1703からカードＩＤを受け取ったデータベース1705では、受け取ったカードIDから対応するユーザ固有情報を検索し、サーバ1703に伝える。サーバ1703は、1716に示すように、ユーザ固有情報を端末1502に伝える。端末1502は、１５１３に示すように、ユーザ固有情報を表示し、ユーザ１７０１に知らせる。ユーザ1701は、表示されたユーザ固有情報が正しいものであるかどうかを見て、判断し、正しい場合には、1718に示すように、暗証番号を端末1702に入力する。

【００７５】図１８は、ＩＣカードを用いた端末の構成図であり、認証を行う際に、本発明が適用できることを示した。

【００７６】端末1801とＩＣカード1809からなる。端末1801には、ＩＣカードを接続するためのカードI/Fを備えている。CPU 1802は、プログラム実行を行い、端末としての表示、入力を行うと共に、ＩＣカードに対する情報の入出力の指示、実行動作等を指定することができる。

【００７７】一方、ＩＣカード1809には、情報を格納するための不揮発性メモリ1813と、情報の入出力制御や、暗号化、復号化の処理に必要なCPU 1810やメモリ1811、そして、端末1801とデータの授受を行うためのカードI/F 1812を備える。

【００７８】図１９は、ＩＣカードでの認証による処理を行なうため、ユーザ、端末、ＩＣカード、そして、ＩＣカード内の不揮発性メモリとの間での処理の流れを示した図である。

【００７９】ユーザ1901が、1905に示すように、カードを端末1902に挿入すると、端末1902は、1906が示すように、挿入されたＩＣカード内のユーザ固有情報の読み出し指示をＩＣカード1903に対して行う。ＩＣカードは、その内部の不揮発性メモリ1904に対して、1907のように、ユーザ固有情報の読み出し指示を行う。ＩＣカード内の不揮発性メモリ1904は、ユーザ固有情報を読み出し、1908のように、ＩＣカード1903に、ユーザ固有情報を渡す。ＩＣカード1903は、1909に示すように、ユーザ固有情報を端末1902に伝える。端末1902は、1910に示すように、ユーザ固有情報を表示し、ユーザ1901に知らせる。ユーザ1901は、表示されたユーザ固有情報が正しいものであるかどうかを見て、判断し、正しい場合には、1911に示すように、暗証番号を端末1902に入力する。端末1902は1912に示すように、暗証番号をＩＣカード1903に伝える。

【００８０】一方、ＩＣカード1903は、1913に示すように、ＩＣカード内の不揮発性メモリ1904に対して、登録されている暗証番号を読み出すように指示を出す。1914のように、不揮発性メモリから読み出された暗証番号は、ＩＣカード1903に渡される。ＩＣカード1903は、端末1902から受け取った暗証番号と、不揮発性メモリ1904から読み出された暗証番号の照合処理を行う。照合結果は1915のように、ＩＣカード1903から、端末1902に伝われ、一致している場合には、1916に示すように、端末1902とＩＣカード1903との間で、決済処理が行われる。

【００８１】

【発明の効果】ユーザが暗証番号を入力する前に、接続したサーバから、ユーザにしかわからないユーザ固有の情報をユーザに対して表示することで、ユーザは正しいシステムであることを確認できるので、安心して、暗証番号を入力することができる。これにより、ユーザが不正な端末やシステムとは知らずに、暗証番号を入力してしまい、暗証番号が盗まれてしまうことを未然に防ぐことができる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すシステム構成図。

【図２】端末およびサーバの構成図。

【図３】端末画面を示した図。

【図４】処理の流れを示した図。

【図５】ユーザ情報管理テーブル。

【図６】「ユーザ」のフローを示した図。

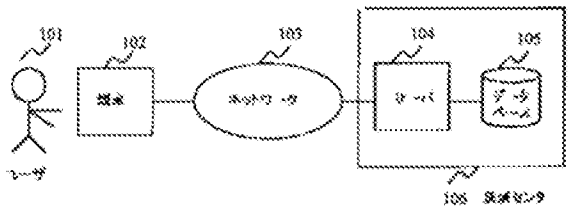
【図７】「端末」のフローを示した図。

【図８】「サーバ」のフローを示した図。

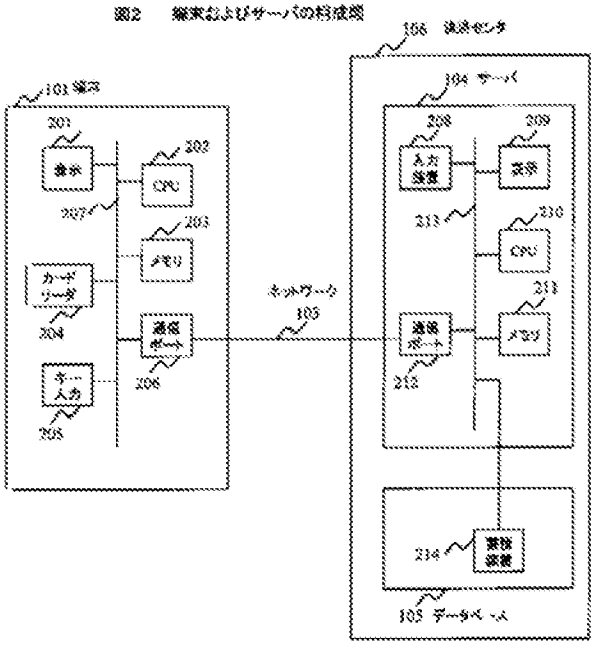
【図9】「データベース」のフローを示した図。
【図10】偽端末の場合に不正を判断する流れを示した図。
【図11】偽サーバへの接続の場合に不正を判断する流れを示した図。
【図12】音声で確認する場合の端末およびサーバの構成図。
【図13】ユーザ固有情報が複数の場合のユーザ情報管理テーブル。
【図14】ユーザ固有情報が複数の場合の端末画面を示した図。
【図15】ユーザ固有情報が複数の場合の処理の流れを示した図。
【図16】認証局を含めたシステム構成図。
【図17】認証局経由の場合の処理の流れを示した図。
【図18】ICカードを用いた端末の構成図。
【図19】ICカードでの認証による処理の流れを示した図。

【符号の説明】
101…ユーザ、102…端末、103…ネットワーク、104…サーバ、105…データベース、106…決済センタ、301a~301d…端末の画面、500…ユーザ情報テーブル、501…ユーザ識別ID、502…ユーザ固有情報、503…暗証番号

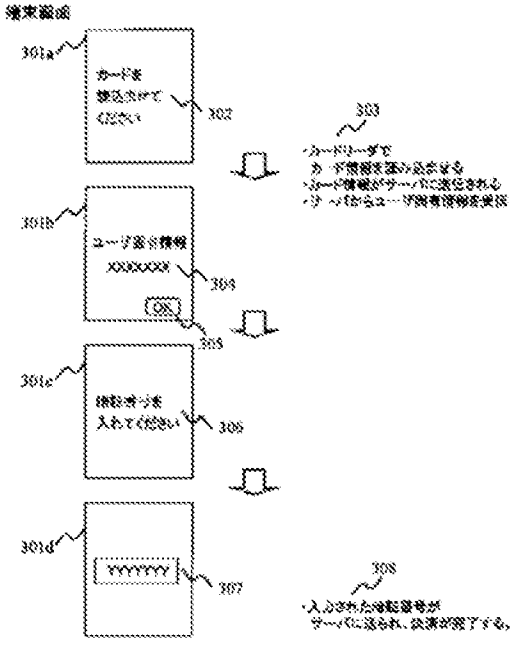
【図1】



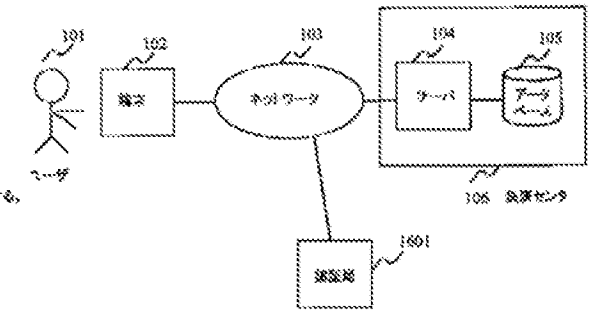
【図2】



【図3】

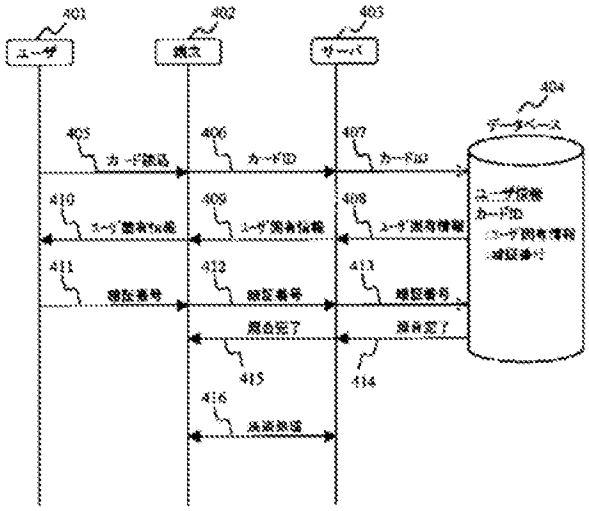


【図16】



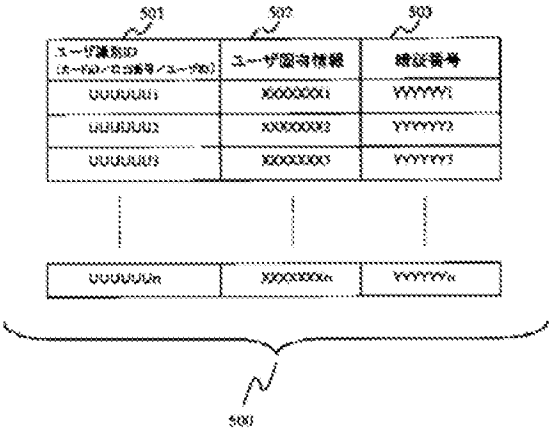
【図4】

図4　処理の流れ



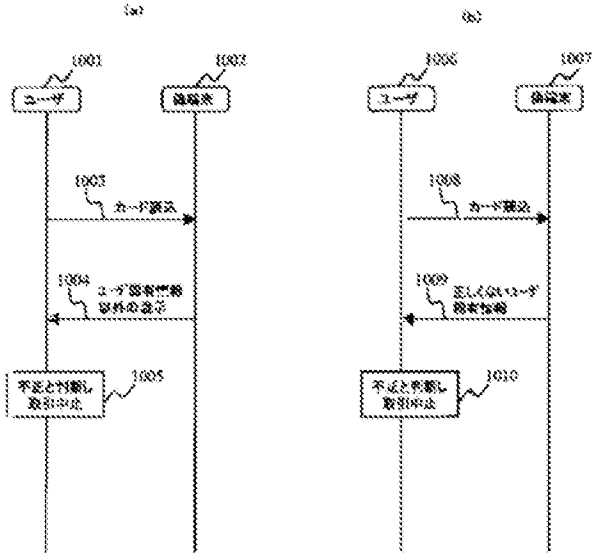
【図5】

図5　ユーザ情報管理テーブル



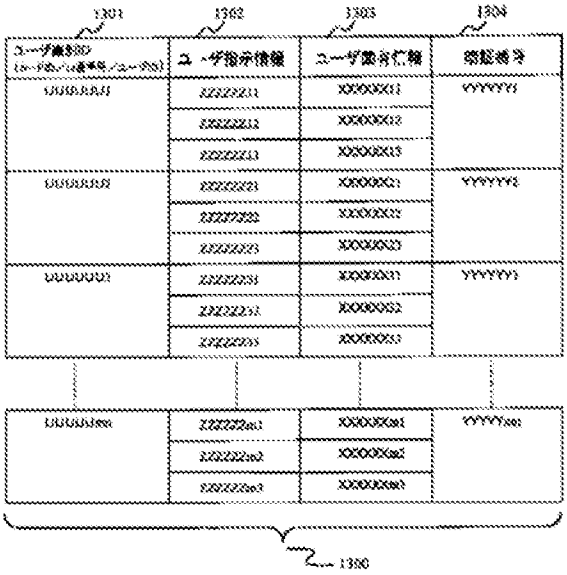
【図10】

図10　偽端末の場合



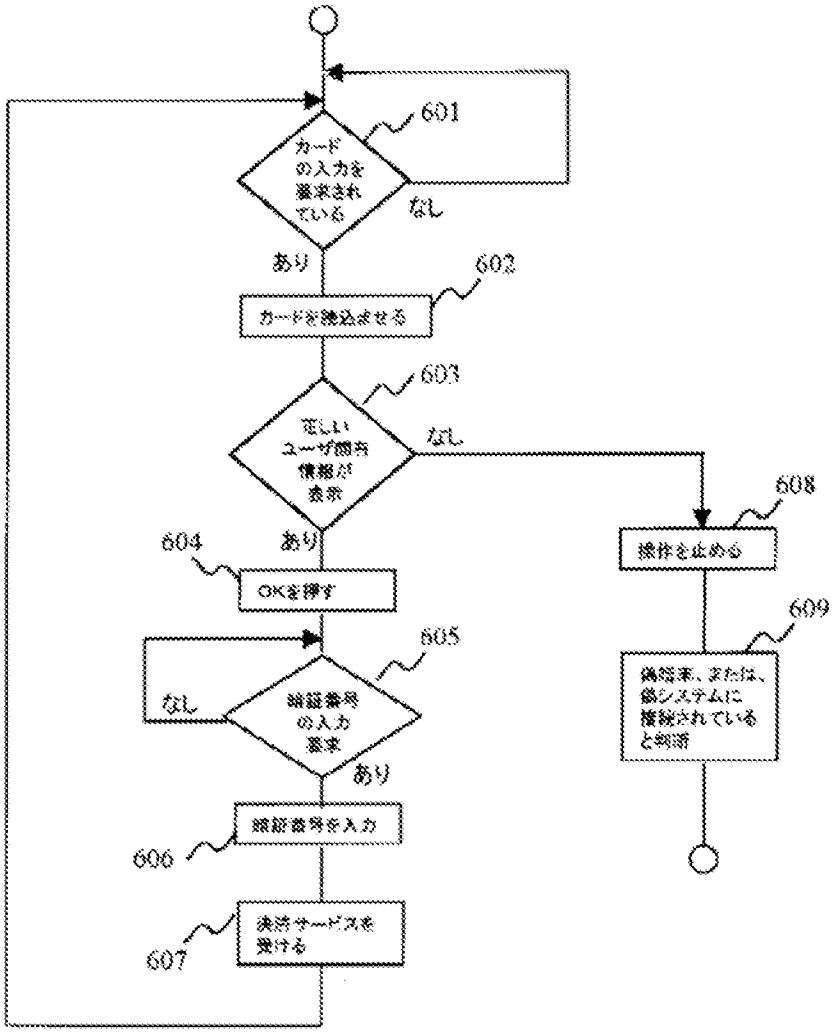
【図13】

図13　ユーザ照合情報が複数の場合の
ユーザ情報管理テーブル



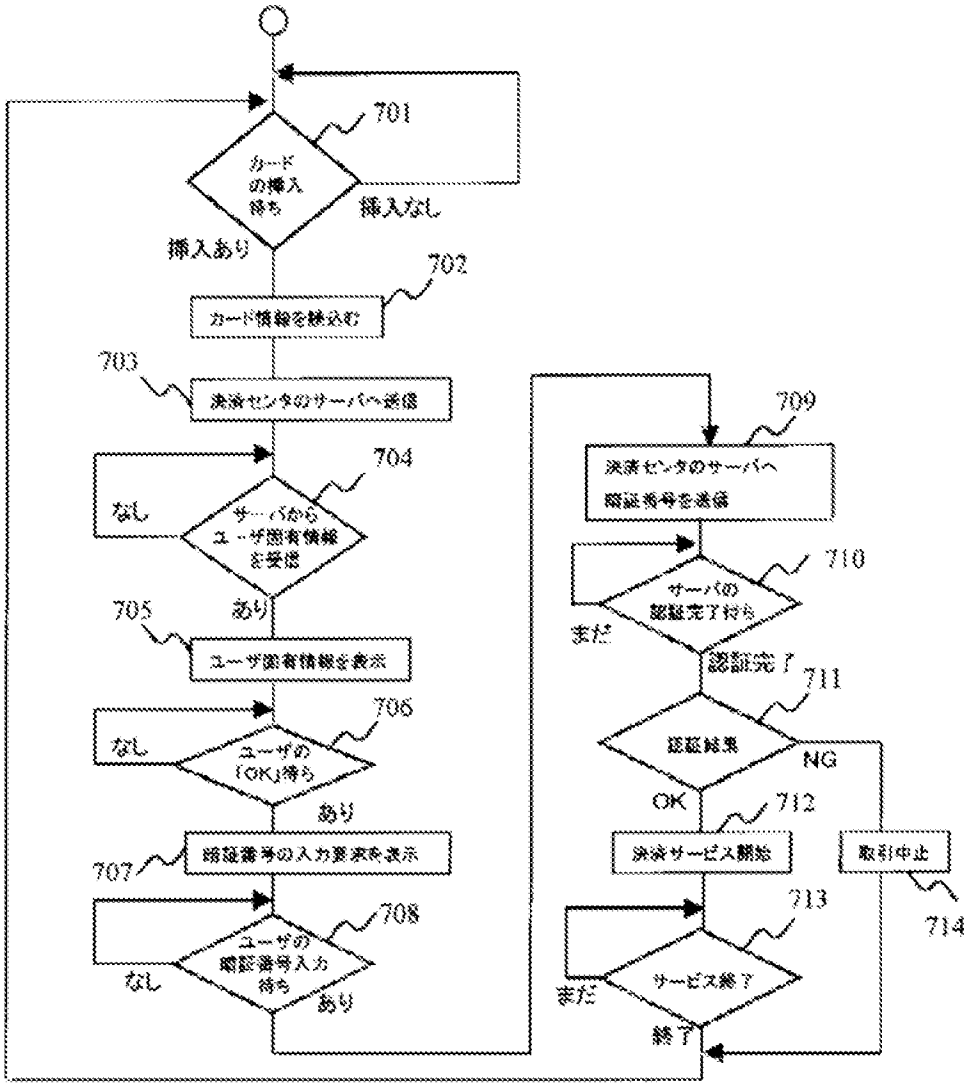
【図6】

図6　「ユーザ」のフロー



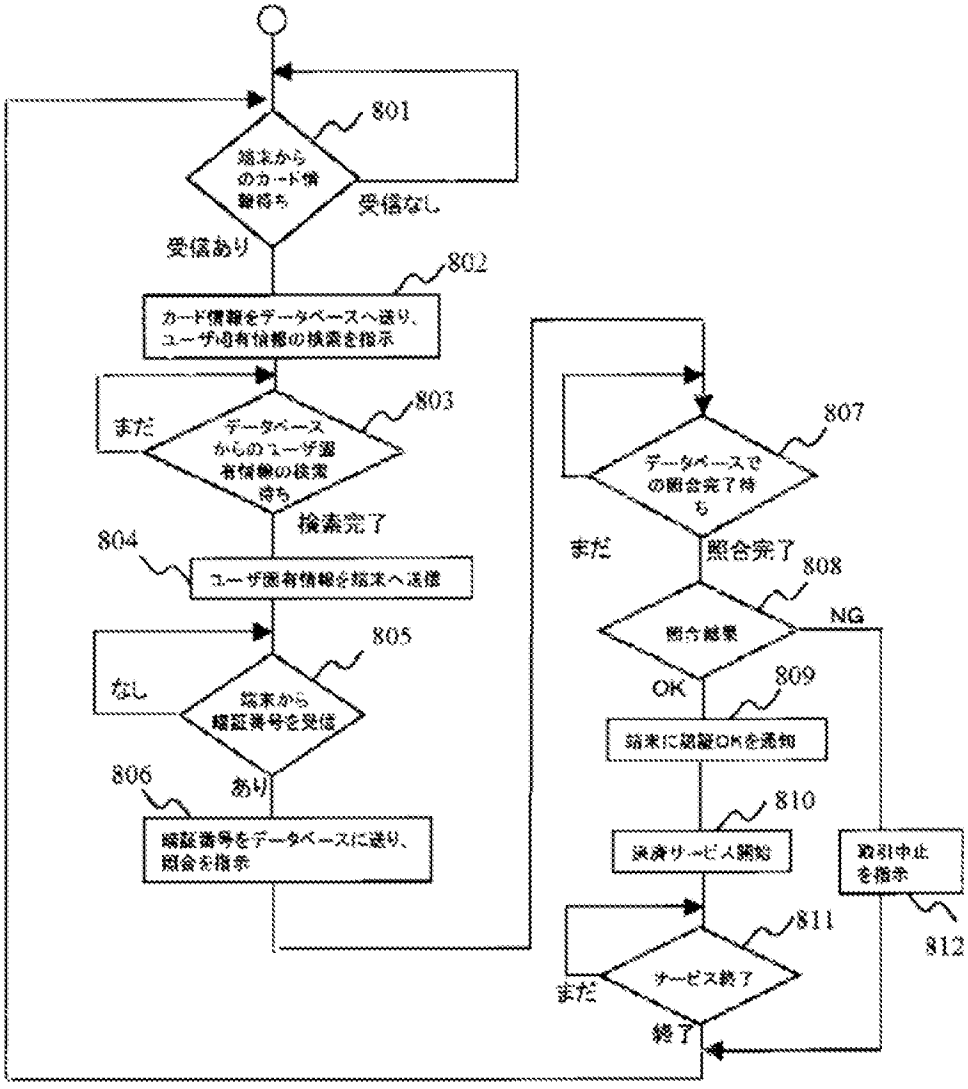
【図7】

図7　「端末」のフロー


701
カードの挿入待ち
挿入なし
挿入あり
702
カード情報を読込む
703
決済センタのサーバへ送信
704
サーバからユーザ固有情報を受信
なし
あり
705
ユーザ固有情報を表示
706
ユーザの「OK」待ち
なし
あり
707
暗証番号の入力要求を表示
708
ユーザの暗証番号入力待ち
なし
あり
709
決済センタのサーバへ暗証番号を送信
710
サーバの認証完了待ち
まだ
認証完了
711
認証結果
NG
OK
712
決済サービス開始
取引中止
714
713
サービス終了?
まだ
終了

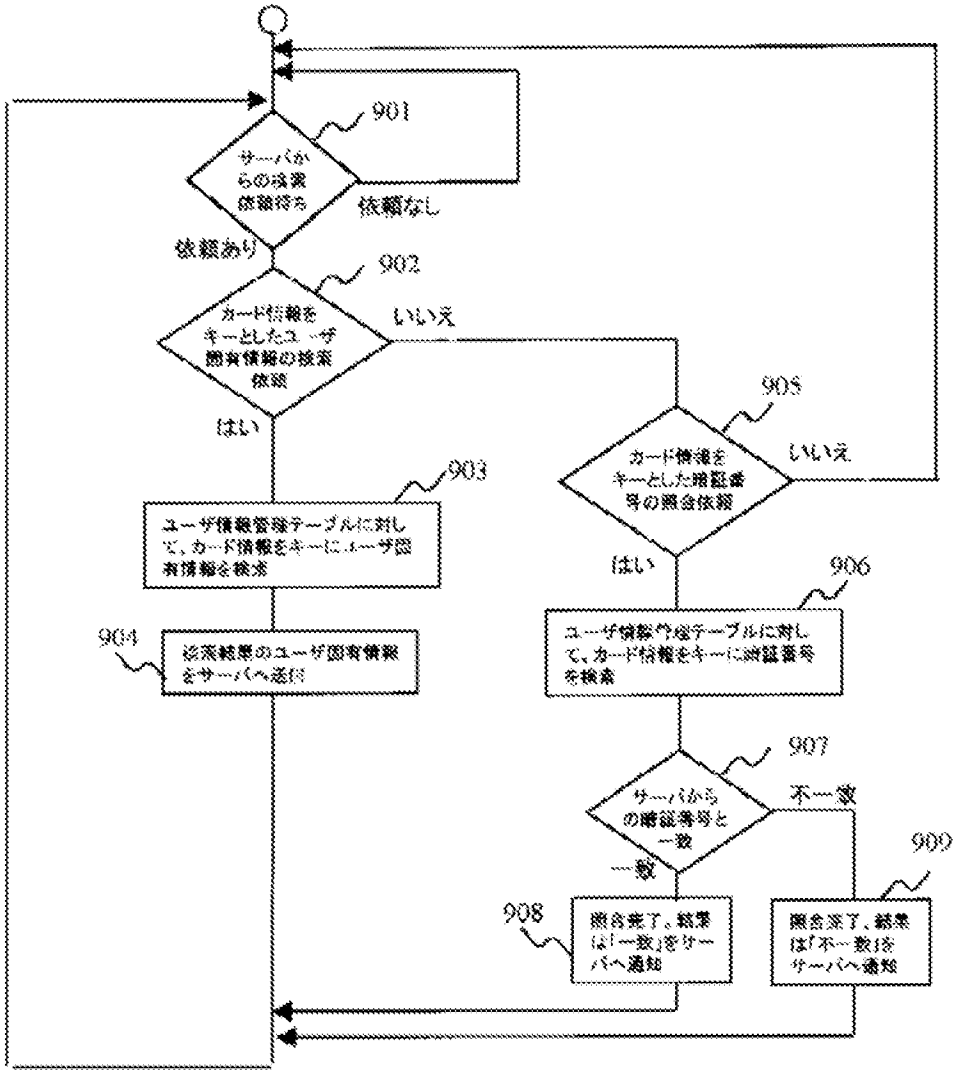
【図8】

図8　「サーバ」のフロー



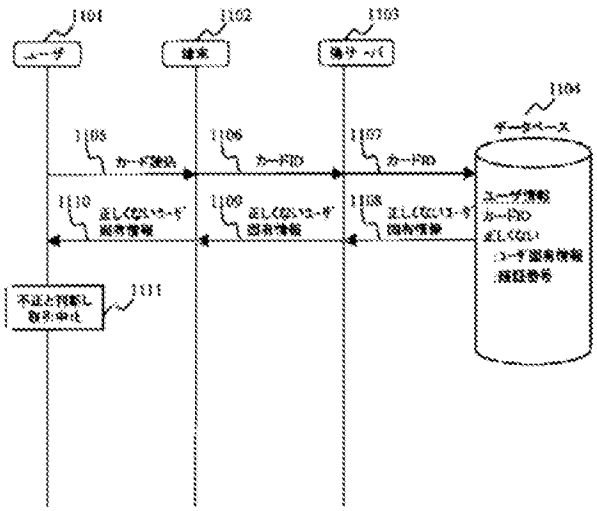
【図9】

図9　「データベース」のフロー



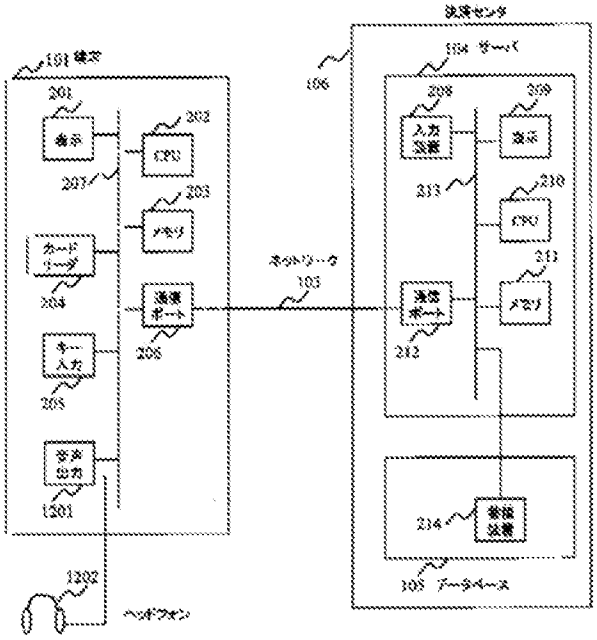
【図11】

図11 各サーバーの処理の流れ



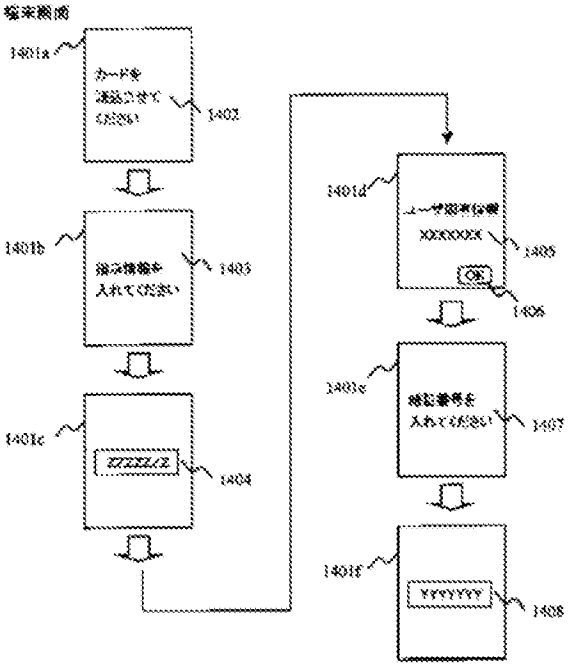
【図12】

図12 音声で認証する場合の端末およびサーバの構成図



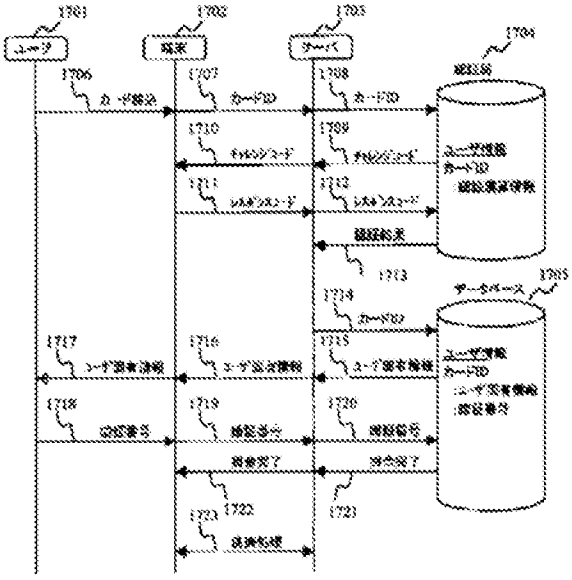
【図14】

図14 ユーザ認証情報が複数の場合の端末画面



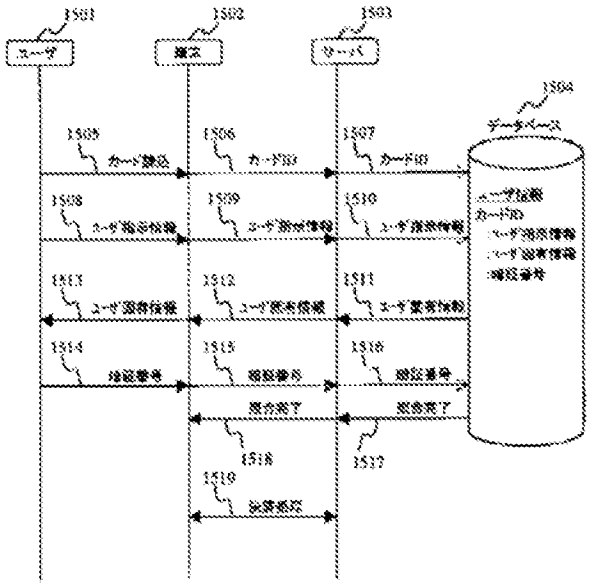
【図17】

図17 認証失敗時の場合の処理の流れ



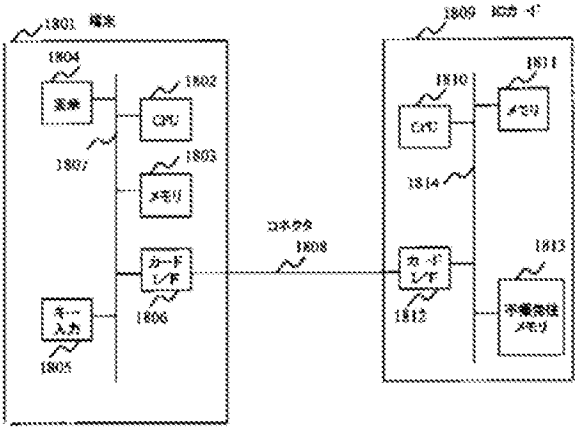
【図15】

図15　ユーザ固有情報が複数の場合の処理の流れ



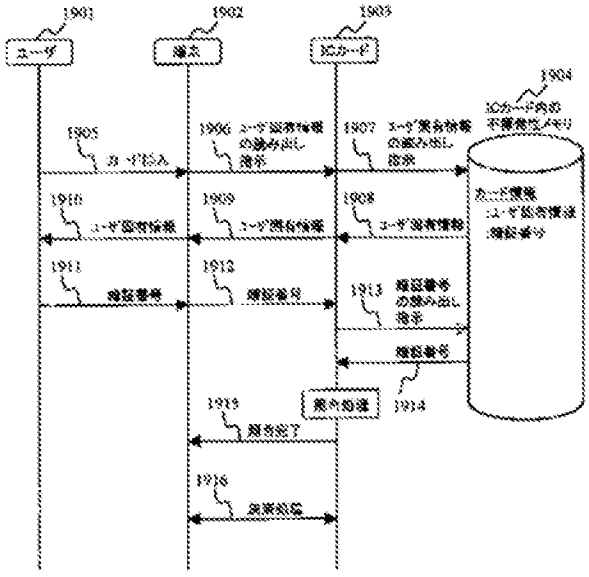
【図18】

図18　ICカードを用いた端末の構成図



【図19】

図19　ICカードでの認証による処理の流れ



フロントページの続き

Fターム(参考) 3K040 AA03 BA18 CA06 CB04 DA03
5B055 BA04 BA15 BA17 JJ05
5B085 AE02 AE03 AE23 AE29
9A001 BB01 BB03 BB04 BB05 CC07
DD13 EE03 FF03 HH15 JJ27
JJ67

Computer-Generated Translation of Specification of JP 2001-117873 A

CLAIMS

[Claim(s)]

[Claim 1]It is a terminal for attesting a terminal user using the 1st information inputted by terminal user, An output means which outputs the 3rd information that said terminal user grasps beforehand according to the 2nd information inputted by said terminal user inputted before a terminal user inputs said 1st information, A terminal, wherein it has an input means which enables an input of said 1st information from said terminal user after said output means outputs the 3rd information, and said output means outputs said terminal user's authentication result based on the 1st information inputted from said input means.

[Claim 2]In the terminal according to claim 1, said 1st information is a password or a password.
A terminal, wherein said 2nd information is user-identification ID which is the information which specifies said terminal user and said 3rd information is user characteristic data as which said terminal user may grasp beforehand correspondence relation between said 2nd information and said 3rd information.

[Claim 3]In the terminal according to claim 2, said 3rd information, Consist of two or more user characteristic data to each terminal user, and said input means inputs directions information which directs one user characteristic data from said two or more user characteristic data from said terminal user, A terminal, wherein said output means outputs user characteristic data chosen based on directions information from said input means.

[Claim 4]A terminal characterized by said output means being what displays said user characteristic data in the terminal according to claim 2.

[Claim 5]Information processing equipment connected to a terminal which attests a terminal user via a network using the 1st information inputted by terminal user, comprising:
A memory measure which constructs two or more 3rd information corresponding to said 1st information, and memorizes it.
A means to retrieve the 3rd information that said terminal user grasps beforehand according

to the 2nd information received from said terminal before said terminal user inputted said 1st information.
A means to transmit said 3rd retrieved information to said terminal.
A means which attests said terminal user using said 1st information received from said terminal after outputting said 3rd information to said terminal.

[Claim 6]In the terminal according to claim 5, said 1st information, Are a password or a password and said 2nd information, It is user-identification ID which is the information which specifies said terminal user, and said 3rd information is user characteristic data as which said terminal user may grasp beforehand correspondence relation between said 2nd information and said 3rd information, Information processing equipment, wherein said memory measure has memorized two or more user characteristic data to each terminal user and said search means searches one of said two or more user characteristic data according to directions information received from said terminal.

[Claim 7]Have the following, and said terminal inputs the 2nd information in advance of an input of said 1st information from said terminal user, transmit to said information processing equipment, and said information processing equipment, It has a memory measure which constructs two or more 3rd information corresponding to said 2nd information, and memorizes it, According to said 2nd information received from said terminal, the 3rd information that said terminal user grasps beforehand is retrieved, A terminal which transmitted said searched result to said terminal, and received said 3rd retrieved information, A user authentication system, wherein said information processing equipment which received the 1st information from said terminal user, transmitted to said information processing equipment, and received the 1st information from said terminal attests said terminal user based on said 1st information.
A terminal into which are a user authentication system which attests a terminal user, and said terminal user is made to input said 1st information using the 1st information inputted by terminal user.
Information processing equipment connected to said terminal via a network.

[Claim 8]In the user authentication system according to claim 7, said 1st information, Are a password or a password and said 2nd information, A user authentication system, wherein it is user-identification ID which is the information which specifies said terminal user and said 3rd information is user characteristic data as which said terminal user may grasp beforehand correspondence relation between said 2nd information and said 3rd information.

[Claim 9]A user authentication method telling said user about said terminal being genuine before a user enters a password or a password into a terminal.

[Claim 10]a password or a password entered by user -- it being the user authentication method which attests a user, and, In advance of an input of said password or a password, user-identification ID from said user is inputted from said user, Constructed two or more user characteristic data corresponding to said password or a password, and they are memorized, According to said user-identification ID, user characteristic data which said user grasps beforehand are searched, A user authentication method receiving a password or a password from said user, and attesting said user based on said received password or a password after outputting as a display said user can recognize said searched user characteristic data to be, or a sound.

[Claim 11]In Claim 9 or a user authentication method of any of 10, or a description, two or more said user characteristic data are memorized to each user.
A user authentication method characterized by choosing one of said two or more user characteristic data based on directions information inputted by said each user.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]When especially this invention attests the user at the time of performing data communications and accessing a server from the computer used as a terminal about data communications, it is concerned with the method, the terminal, server, and system which check the justification of the computer which a user uses, or a server.
[0002]
[Description of the Prior Art]Conventionally, in the system which consists of a terminal and a server, it was performed that a server attests whether it is regular for a terminal or its user or that a terminal attests whether the server of a connection destination is a right server.
[0003]For example, in the exchange between a terminal and a server, the device which confirms mutually whether a terminal and a server are right things made the user input one of the passwords prepared beforehand, checked mutual justification and suited as indicated to JP,H11-85702,A.
[0004]There was a device with which a third party does not try to be robbed of a password or a password at the time of an input conventionally.

[0005]For example, in a cash automatic transaction machine, they are card information and the combination of a password, The method of carrying out user authentication was common, and changed the display or key operation was kept from being known, and when inputting a password as indicated to JP,H11-191094,A, it was devised so that others might not try to be robbed.

[0006]

[Problem to be solved by the invention]Mutually in a check method whether the above, a terminal, and a server are right things, Since the user who inputs a password was not able to check correctly whether it is connected to a right server, or a terminal is regular, it is that the machine itself is imitation and had not become management to the danger that a password will be stolen.

[0007]In a device with which a third party does not try to be robbed of a password or a password at the time of an input, since, as for the cash automatic transaction machine, saying [that it is a right machine] was the requisite, the user trusted the machine, and he had inputted the password as he followed the directions. Therefore, there was no management to the danger that a password will be stolen because the machine itself is imitation.

[0008]Although a variety of terminals are used at a taxi and various places, such as an extraordinary store, and the cases where settling processing is performed will increase in number especially from now on, A user whether the terminal, or the server and system which are connected are a right thing. Or it cannot be detected by the method of inserting the present card and inputting a password as it is whether it is the fake terminal or fake system made in order to steal card information and a password.

[0009]In the electronic banking by Electronic Commerce Technology Division or a debit card, since the server linked to a terminal or a terminal is imitation, the purpose of this invention is to provide the identifying method, the terminal, server, and system which prevent beforehand that a password will be stolen by others.

[0010]

[Means for solving problem]To achieve the above objects, in this invention by the input of insertion of a card, user ID, an account number, etc. A means for the means which gives that information to a server, and a server to transmit to a terminal the information peculiar to a user which only a user understands from this input, and to display, A user is recognizing it being heard and their being the contents of the right, or it sees reading the transmitted information peculiar to a user, after he checks that a terminal and a server are just, inputs a password and forms a means to transmit to a server.

[0011]That is, before inputting a password not to leak to others, it solves by preparing the mechanism in which a system provides the information a user judges it to be whether this

terminal and a system are regular. When a user displays the information peculiar to a user registered into the regular server on a terminal and shows it beforehand to a user as information for the judgment, a user enables it to judge a regular thing and imitation.

[0012]

[Mode for carrying out the invention]Hereafter, an embodiment of the invention is described using Drawings.

[0013]Drawing 1 is a system configuration figure showing one embodiment of this invention.

[0014]In this figure, the database with which a terminal and 103 store a network, 104 stores a server, and, as for 101, a user and 102 store User Information, as for 105, and 106 show a settlement center.

[0015]When the user 101 uses the terminal 102 and performs settling processing from a remote place, The network 103 is used, the server 104 in the settlement center 106 is accessed, and after performing authenticating processing using the database 105 with which the user's information is accumulated, settlement of accounts is processed. It is using a card and entering a password or a password (it is only hereafter described as a password) in this example, mainly when a user's performs settling processing, The server of a settlement center is reached, and by comparing with the registration data in a server, the information proves that he is the person himself/herself, and performs settling processing.

[0016]Drawing 2 shows the terminal and the server block diagram.

[0017]As shown in this figure, the terminal 101 has the display 201, CPU 202, the memory 203, the card reader 204, the key input section 205, and the communication port 206. The settlement center 106 is provided with the following.

Server 104.

Database 105.

The server 104 has the input device 208, the display 209, CPU 210, the memory 211, and the communication port 212. The database 105 comprises the storage device 214. The server 104 and the database 105 are connected by bus 213. The terminal 101 and the server 104 are connected in the network 103.

[0018]CPU 202 executes the program currently stored in the memory 203, and the terminal 101 performs control of the card reader 204, display by the display 201, input from the keystroke 205, and communication with the server which leads the communication port 206.

[0019]CPU 210 executes the program currently stored in the memory 211, and the server 104 performs communication with the terminal which leads the communication port 206, access to the database 105, the display by the display 209, and the input from the input device 208.

[0020]The database 105 is a basis of the program execution in the server 104, and performs

search of data and collation.

[0021]Drawing 3 is a figure showing a screen display in the terminal which applied this invention.

[0022]301 d of screen display in alignment with a flow of processing is shown from the terminal screen 301a. In the terminal screen 301a, the display 302 of "let me read a card" appears in the beginning. Thereby, a user makes card information read by a card reader of a terminal as shown in 303. Next, card information is transmitted to a server and user characteristic data searched from a database from this card information are sent to a terminal from a server. If the user characteristic data 304 are displayed, a user judges this to be a right value and OK button 305 is pushed as shown in the terminal screen 301b, a screen will change to the terminal screen 301c. The display 306 "put in a password" comes out in the terminal screen 301c.

[0023]Thereby, a user inputs the password 307, as shown in the terminal screen 301d.

[0024]Then, as shown in 308, an inputted password is sent to a server and settling processing is performed. In the terminal screen 301a, after insertion of a card is directed, in the terminal screen 301b, it is shown in user characteristic data being displayed. A user looks at these displayed user characteristic data, and it judges whether it is what he registered into a settlement center a priori, and only when it is a right value, a password is called input at the terminal 301d.

[0025]Although the screen which directs the input of a password came out as it is here, without displaying user characteristic data or user characteristic data were displayed, Since a user can judge that the terminal currently used or the connected server is inaccurate and it is not necessary to input a password when the displayed value is wrong, it can prevent that a password is stolen.

[0026]Drawing 4 is a user, a terminal, a server, and a figure showing the flow of processing between databases.

[0027]If the user 401 makes a card read into the terminal 402 as shown in 405, a terminal will tell card ID within the read card information to the server 403, as shown in 406. Here, card ID should just be a name, a sign, a number, etc. which are the information which can specify a user. Card ID functions in this meaning as user-identification ID including concepts shown in drawing 5, such as an account number and user ID.

[0028]The server 403 tells card ID to the database 404, as shown in 407. From User Information accumulated, user characteristic data are searched with the database 404 to a key, and in it, card ID is told to the server 403, as shown in 408. Here, user characteristic data are information, including a name, a number, a sign, a sound, etc., which is uniquely specified by previous user-identification ID and is beforehand recognized by the user.

[0029]The server 403 gives user characteristic data to the terminal 402, as shown in 409. As

shown in 410, the terminal 402 displays user characteristic data and tells the user 401 about them. The user 401 judges seeing the displayed user characteristic data whether be a right thing, and as shown in a right case 411, he inputs a password into the terminal 402. The terminal 402 tells a password to the server 403, as shown in 412. The server 403 tells a password to the database 404, as shown in 413. In the database 404, the told password compares whether it is in agreement with the password beforehand registered into User Information in a database. When in agreement, as shown in 414, it is reported to the server 403 that a result is the notice of the completion of collation. In the server 403, as shown in 415, when it notifies the completion of collation to the terminal 402 and is in agreement, the settling processing 416 is started in the terminal 402 and the server 403.

[0030]drawing 5 is the User Information management table accumulated in the database in a settlement center -- it becomes user-identification ID 501 and the user characteristic data 502 from the password 503.

[0031]User-identification ID 501, card ID, an account number, user ID, etc. are used, for example. This User Information management table 500 can search now the user characteristic data 502 and the password 503 for user-identification ID 501 to a key.

[0032]Drawing 6 is a figure showing the process flow seen from the "user" in this invention.

[0033]602 a user makes a card read into from a terminal in the processing 602 in the processing 601 when there is a demand of an input of a card. Next, in the processing 603, the user characteristic data which a terminal displays are seen whether be a right thing, and it judges, and if right, an OK button will be pushed in the processing 604. Next, like the processing 605, if a terminal asks for the input of a password, in the processing 606, it will input a password and will receive account settlement services in the processing 607 after that.

[0034]When the information which user characteristic data were not displayed or was displayed in the processing 603 on the other hand is not a right thing, Processing is finished in the processing 608, without stopping operation, the used terminal being a fake terminal, or judging that it is connected to a fake system like the processing 609, and inputting a password.

[0035]Drawing 7 is a figure showing the process flow performed with the "terminal" in this invention. The function shown here is realized as a program.

[0036]In the processing 701, if insertion waiting of the card is carried out and there is card insertion, in the processing 702, the card information containing user-identification ID will be read. The read card information is transmitted to the server of a settlement center in the processing 703. Next, in the processing 704, if there are waiting and reception about reception of user characteristic data from a server, in the processing 705, user characteristic data will be displayed on the screen of a terminal. Next, if a user pushes the button of O.K.

as shown in the processing 706, in the processing 707, the input request of a password will be displayed on a terminal screen to a user. In the processing 708, when there is an input of the password by a user, in the processing 709, the password inputted into the server of the settlement center is transmitted. Next, in the processing 710, the result of the attestation of the completion of attestation by a server by the processing 711 waiting and when it completes is investigated, and if it is O.K., and account settlement services are made to start and service is completed in the processing 713 in the processing 712, it will return to the first state.

[0037]On the other hand, in the processing 711, when an authentication result is NG, like the processing 714, the measure of a dealings stop is taken and it returns to the first state.

[0038]Drawing 8 is a figure showing the process flow performed by the "server" in this invention. The function shown here is realized as a program.

[0039]In the processing 801, receiving waiting of the card information containing user-identification ID from a terminal is performed, when it receives, in the processing 802, the received card information is sent to a database and search of user characteristic data is directed. Next, in the processing 803, search waiting of the user characteristic data from a database is performed, and transmission to the terminal of the searched user characteristic data is performed in the processing 804 at the time of the completion of search. Next, in the processing 805, if there are waiting and reception about the password from a terminal, in the processing 806, the password which received is sent to a database and the collation processing of whether to be in agreement with the password beforehand registered into the database is directed. In the processing 807, when it turns out that the collation processing in the database was completed, in the processing 808, a matching result is investigated, and if it is O.K., and account settlement services are made to start and service is completed in the processing 811 in the processing 810, it will return to the first state.

[0040]On the other hand, in the processing 808, when a matching result is NG, a measure of issuing directions of a dealings stop is taken like the processing 812, and it returns to the first state.

[0041]Drawing 9 is a figure showing a process flow of a "database" in this invention. A function shown here is realized as a program.

[0042]In the processing 901, when there are waiting and a request, retrieval requesting from a server, In the processing 902, it investigates whether it is the retrieval requesting of user characteristic data to which the contents of the request used as a key card information containing user-identification ID, and when that is right, in the processing 903, card information is retrieved for user characteristic data to a key to the User Information management table. And in the processing 904, user characteristic data of search results are transmitted to a server, and it returns first.

[0043]On the other hand, when a request content is not search of user characteristic data in the processing 902, it is investigated whether it is having been the collation request of a password which used as a key card information in which a request content includes user identification information in the processing 905. When that is right, card information is retrieved for a password by the processing 906 to a key to the User Information management table. And in the processing 907, it investigates whether a password from a server and a searched password are in agreement, and in being in agreement, in the processing 908, collation completion processing is performed, and it notifies a server that a matching result is "coincidence", and returns first.

[0044]On the other hand, in the processing 907, when the password from a server and the searched password are not in agreement, in the processing 909, collation completion processing is performed, and it notifies a server that a matching result is "disagreement", and returns first.

[0045]In the processing 905, when a request content corresponds to neither, it returns first.

[0046]It is a figure showing the flow of processing until it judges that drawing 10 is inaccurate when the terminal currently used is a fake terminal and comes to stop dealings.

[0047]. The user 1001 makes a card read into the terminal (fake terminal) 1002 like 1003. Like 1004, since the user characteristic data which cannot be connected to a regular server, either but should be returned since a terminal is imitation are not known, either, when the display of those other than user characteristic data is performed, in the processing 1005, a user judges that it is inaccurate and stops dealings.

[0048]. The user 1006 makes a card similarly read into the terminal (fake terminal) 1007 like 1008. Like 1009, since the user characteristic data which cannot be connected to a regular server, either but should be returned since a terminal is imitation are not known, either, when the user characteristic data which are not right are displayed, in the processing 1010, a user judges that it is inaccurate and stops dealings.

[0049]It is a figure showing a flow of processing until it judges that drawing 11 is inaccurate when a connected server is a fake server and comes to stop dealings. The fake server cannot access a database regular as a matter of course. Therefore, the fake server cannot grasp a relation of user-identification ID and user characteristic data as shown in drawing 5, and cannot search regular user characteristic data from card ID received from the terminal 1102.

[0050]The user 1101 makes a card read into the terminal 1102 like 1105. Although the terminal 1102 tells user-identification ID, such as card ID, like 1106 to the connected server (fake server) 1103, and the fake server 1103 tends to receive this and tends to search user characteristic data with the database 1104, Since a right value is not registered, user characteristic data which are not right get across to the fake server 1103 like 1108. Further,

the fake server 1103 gives these user characteristic data that are not right to the terminal 1102 like the processing 1109, and like the processing 1110, the terminal 1102 displays those user characteristic data that are not right in a display of a terminal, and it urges processing to it at a user. Like the processing 1111, the user 1101 judges that it is inaccurate and takes a measure of a dealings stop.

[0051]An embodiment shown below is an embodiment in a case of telling a user about user characteristic data with a sound.

[0052]With a sound, drawing 12 is a terminal or a terminal in a case of identifying whether a connected server is a genuine article or imitation, and a block diagram of a server, and comprises the terminal 101, the settlement center 106, the server 104, and the database 105.

[0053]The terminal 101 is equipped with the voice output part 1201, and the headphone 1202 can be connected now to this. In CPU 202 of a terminal, user characteristic data received from the server 104 are changed into a sound, and are reproduced by the voice response 1201, and it is judged whether users are right user characteristic data. The headphone 1202 are for read-out information not being heard by the 3rd person.

[0054]When there is only no screen display in a terminal and a sound also enables it to view and listen to it, it becomes a system which is easy to use also for a visually impaired person.

[0055]An embodiment shown below is an embodiment at the time of enabling it to register two or more user characteristic data, being able to change a verifying means if needed, and improving safety.

[0056]Drawing 13 is a figure showing the User Information management table accumulated in a database in case user characteristic data are plurality, and serves as user-identification ID 1301, the user instruction information 1302, and the user characteristic data 1303 from the password 1304.

[0057]User-identification ID 1301, card ID, an account number, user ID, etc. are used, for example. Which user characteristic data are read by the ability to register two or more user characteristic data to one user-identification ID is that a user specifies the user instruction information 1302, and the user characteristic data 1303 corresponding to it are read. That is, about the user characteristic data 1303, user-identification ID 1301 and the user characteristic data 1303 which the user instruction information 1302 serves as a key, and search is performed, and correspond are read.

[0058]Since two or more user characteristic data are prepared and it can specify for the user presentation information 1302, Since a user has in a terminal a means to check whether it is a regular thing, using other user characteristic data even if user characteristic data should be known by others, since the value used for a check can be changed now if needed, his safety improves. When it is judged that the user characteristic data currently used usually were stolen, it becomes possible to prevent being stolen to a password by enabling it to choose

another user characteristic data by user instruction information.

[0059]Drawing 14 is a figure showing a terminal screen in case user characteristic data are plurality.

[0060]After making a card read from the terminal screen 1401a in the terminal screen 1401f, in order to make a user display the user characteristic data which a user means, the input of directions information is urged and the user characteristic data which suited the directions information are displayed after that.

[0061]In the terminal screen 1401b, Screen 1403 to which the input of directions information is urged is displayed after a card input, and a user inputs the directions information 1404 in the terminal screen 1401c. Thereby, in the terminal screen 1401d, the corresponding user characteristic data 1405 are displayed and the user can judge whether it is a regular thing.

[0062]Drawing 15 is a figure showing the flow of processing in case there are two or more user characteristic data.

[0063]A flow of processing between a user, a terminal, a server, and a database is shown.

[0064]If the user 1501 makes a card read into the terminal 1502 as shown in 1505, a terminal will tell card ID within read card information to the server 1503, as shown in 1506. The server 1503 tells card ID to the database 1504, as shown in 1507.

[0065]If the user 1501 inputs user instruction information into the terminal 1502 as shown in 1508, a terminal will give inputted user instruction information to the server 1503, as shown in 1509. The server 1503 gives inputted user instruction information to the database 1504, as shown in 1510.

[0066]From User Information accumulated, user characteristic data are searched with the database 1504 to a key, and in it, card ID and user instruction information are given to the server 1503, as shown in 1511. The server 1503 gives user characteristic data to the terminal 1502, as shown in 1512. As shown in 1513, the terminal 1502 displays user characteristic data and tells the user 1501 about them. The user 1501 judges seeing displayed user characteristic data whether be a right thing, and as shown in a right case 1514, he inputs a password into the terminal 1502.

[0067]Drawing 16 is a system configuration figure including a certificate authority which this invention applied to authenticating processing including a certificate authority.

[0068]The database with which a terminal and 103 store a network, 104 stores a server, and, as for 101, a user and 102 store User Information, as for 105, and 106 show a settlement center, and 1601 shows a certificate authority.

[0069]When the terminal 102 gives card information to the server 104, after attesting by the certificate authority 1601, it is the example which displayed the user characteristic data of this invention, and a user is a right terminal and enabled it to check having connected with a

right server.

[0070]Drawing 17 is a figure showing the flow of processing in via the certificate authority in the system of drawing 16.

[0071]The flow of processing between a user, a terminal, a server, a database, and a certificate authority is shown.

[0072]If the user 1701 makes a card read into the terminal 1702 as shown in 1706, a terminal will tell card ID within read card information to the server 1703, as shown in 1707. The server 1703 tells card ID to the certificate authority 1704, as shown in 1708.

[0073]In the certificate authority 1704, as authentication arithmetic information is retrieved to a key and card ID is shown in 1709 from User Information accumulated, a generated challenge code is told to the server 1703. The server 1703 tells a challenge code to the terminal 1702, as shown in 1710. As shown in 1711, the terminal 1702 calculates a response code to a challenge code, and returns it to the server 1703. The server 1703 passes a response code from the terminal 1702 to the certificate authority 1704, as shown in 1712. In the certificate authority 1704, a response code received from the server 1703 is investigated, and the server 1703 is passed as an authentication result like 1713. The server 1703 passes card ID previously received from a terminal like 1714 to the database 1705, when it is contents made just [a received authentication result]. Processing is ended without sending card ID received from the terminal 1702 to a database, when it is not contents made just [the contents of the authentication result which the server 1703 received].

[0074]User characteristic data corresponding from received card ID are searched with the database 1705 which received card ID from the server 1703, and it tells the server 1703. The server 1703 gives user characteristic data to the terminal 1502, as shown in 1716. As shown in 1513, the terminal 1502 displays user characteristic data and tells the user 1701 about them. The user 1701 judges seeing displayed user characteristic data whether be a right thing, and as shown in a right case 1718, he inputs a password into the terminal 1702.

[0075]Drawing 18 was a block diagram of a terminal which used an IC card, and when it attested, it showed that this invention was applicable.

[0076]It consists of the terminal 1801 and IC card 1809. The terminal 1801 is equipped with card I/F for connecting an IC card. CPU 1802 performs program execution, and performs a display as a terminal, and an input, and it can specify directions of input and output of information over an IC card, execution operation, etc.

[0077]On the other hand, IC card 1809 is equipped with card I/F 1812 for performing transfer of the nonvolatile memory 1813 for storing information, CPU 1810 and the memory 1811 required for input/output control of information, and processing of encryption and a decoding and the terminal 1801, and data.

[0078]Drawing 19 is a figure showing a flow of processing between nonvolatile memory in

a user, a terminal, an IC card, and an IC card in order to perform processing by attestation by an IC card.

[0079]If the user 1901 inserts a card in the terminal 1902 as shown in 1905, the terminal 1902 will perform read instruction of user characteristic data in an inserted IC card to IC card 1903, as shown in 1906. An IC card performs read instruction of user characteristic data like 1907 to the nonvolatile memory 1904 of the inside. The nonvolatile memory 1904 in an IC card reads user characteristic data, and passes user characteristic data like 1908 to IC card 1903. IC card 1903 gives user characteristic data to the terminal 1902, as shown in 1909. As shown in 1910, the terminal 1902 displays user characteristic data and tells the user 1901 about them. The user 1901 judges seeing displayed user characteristic data whether be a right thing, and as shown in a right case 1911, he inputs a password into the terminal 1902. The terminal 1902 tells a password to IC card 1903, as shown in 1942.

[0080]On the other hand, as shown in 1913, IC card 1903 issues directions so that a password registered may be read to the nonvolatile memory 1904 in an IC card. A password read from nonvolatile memory is passed to IC card 1903 like 1914. IC card 1903 performs collation processing of a password received from the terminal 1902, and a password read from the nonvolatile memory 1904. When a matching result can get across to the terminal 1902 and is in agreement from IC card 1903 like 1915, as shown in 1916, settling processing is performed between the terminal 1902 and IC card 1903.

[0081]

[Effect of the Invention]By displaying the information peculiar to a user which only a user understands from the connected server to a user, before a user inputs a password, since the user can check that it is a right system, he feels easy and can input a password. A user can input a password into not knowing as an inaccurate terminal and system by this, and it can prevent that a password will be stolen.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The system configuration figure showing one embodiment of this invention.

[Drawing 2]A terminal and the block diagram of a server.

[Drawing 3]The figure showing a terminal screen.

[Drawing 4]The figure showing the flow of processing.

[Drawing 5]User Information management table.

[Drawing 6]The figure showing the flow of a "user."

[Drawing 7]The figure showing the flow of a "terminal."

[Drawing 8]The figure showing the flow of a "server."

[Drawing 9]The figure showing the flow of a "database."
[Drawing 10]The figure showing the flow which judges injustice in the case of a fake terminal.
[Drawing 11]The figure showing the flow which judges injustice in connection with a fake server.
[Drawing 12]The terminal in the case of checking with a sound, and the block diagram of a server.
[Drawing 13]The User Information management table in case user characteristic data are plurality.
[Drawing 14]The figure showing a terminal screen in case user characteristic data are plurality.
[Drawing 15]The figure showing the flow of processing in case user characteristic data are plurality.
[Drawing 16]A system configuration figure including a certificate authority.
[Drawing 17]The figure showing the flow of processing in via a certificate authority.
[Drawing 18]The block diagram of the terminal using an IC card.
[Drawing 19]The figure showing the flow of processing by attestation by an IC card.

[Explanations of letters or numerals]
101 [-- A server, 105 / -- A database, 106 / -- A settlement center, 301a-301d / -- The screen of a terminal 500 / -- The User Information table, 501 / -- User-identification ID, 502 / -- User characteristic data, 503 / -- Password] -- A user, 102 -- A terminal, 103 -- A network, 104